Agenda Item 6

Chelmsford City Council

Chelmsford City Council Governance Committee

31 October 2022

Information Governance Update

Report by:

Data Protection Officer

Officer Contact:

John Breen, Information Governance Manager & DPO,
john.breen@chelmsford.gov.uk. 01245 606215

Purpose

To provide an annual update on the Council's approach to the assurance and management of information.

Recommendations

1. To note the contents of this report.

Achievements and Further Developments

1. Statutory Requests – information requests comprise of Freedom of Information, Environmental Information Regulation and Data Protection Act Subject Access requests. In 2021/22 the Information Governance team, together with services, processed 785 requests and 90% were answered within statutory timescales. This compares with 796 requests received in 2020/21 where 85% were answered within timescale. A 5% increase in performance during the last year represents a good improvement for the Council and brings us in line with the overall target of 90%. Furthermore, two cases relating to these information requests were referred to the Information Commissioner's Office (ICO) in 2021/22. These cases have now been resolved.

2. Data Breaches – the number of data breaches increased from 22 in 2020/21 to 27 in 2021/22. These breaches are categorised into 17 email breaches, 6 enveloping breaches and 4 other breaches. All data breaches are investigated thoroughly in line with the Council's Data Breach Procedure. These investigations also enable the Council and officers a chance to learn from these breaches. In addition, no cases relating to data breaches were referred to the ICO in 2021/22.

3. Training and Awareness – the 'human factor' is often the weakest link in information security and therefore ensuring staff are appropriately trained is a very important element of compliance for data protection. In 2018/19, general GDPR eLearning training was delivered to all computer-based staff. A year later a new eLearning course was launched and focussed on cyber awareness. In 2021/22 a new eLearning course on cyber awareness and home working was developed to coincide with the organisational shift towards more individuals working from home. The Council achieved a completion rate of 90% which is above the target set at 85% and ranks very highly for district Councils.

   A new eLearning course is currently being developed which is due to be sent out to staff and Councillors shortly. The course is mainly based on cyber security and offers very good awareness when individuals are online or using email. Email has been specifically targeted this year due to the increase in email data breaches, as well as results from the organisations phishing simulations in recent years.

4. Cyber Security Review – in February 2021, the Council proactively commissioned a Cyber Security Review which identified the progress the Council has made in recent times, as well as identifying areas most in need of improvement. Since then, we have appointed a vCISO (Virtual Chief Information Security Officer), who is a highly trained Cyber Security expert, to work with the authority for 24 days a year to improve security against cyber threats. They are currently assisting the organisation in:
   - communicating cyber risks and how to mitigate against them to Management Team and Members.
   - ensuring the organisation understands that everyone is responsible for information security, and they are not just seen as an IT or Governance issue. Actions will be developed to help the organisation progress with this.
   - progressing with awarding an incident response retainer, similar to recovery insurance, for when we are compromised.
   - The implementation of Microsoft Sentinel. This system will aggregate logs and events from across all the Council infrastructure in real time to allow us (and any third-party security team) to have an overview of any cyber security events or issues.

5. Policies - In June 2021, Management Team agreed a new Acceptable Use Policy. This combines a number of security policies into one overall policy. More

recently, the Council's Information Governance Policy and Breach Policy and Procedures have been updated. In addition, best practice for consultation has also been developed which includes more consistent approaches for Council services capturing sensitive information.

6. Consents – the General Data Protection Regulations (GDPR) introduced more stringent rules around consents, meaning organisations were required to consider how the consents were obtained in order to determine if they were GDPR compliant. The Council has refined its marketing lists to ensure adequate consents under GDPR are in place and have worked on rebuilding its depleted marketing lists. The number of unique subscribers is now over 60,000 as the number of subscribers increased by nearly 9,000 last year. In addition, in the last year, 519 e-marketing campaigns have been sent out to 2.8 million recipients.

7. Privacy Notices – organisations are required to have privacy notices to inform users how they are going to use their data before receiving it. The Council now has 27 privacy notices in place across a range of different service areas, which are regularly reviewed and updated.

8. Risk Management – information governance risks have been developed and fit the Council's revised risk management criteria. They are an important step in the Council's maturing information governance framework and enable the Council to put more effort and resources into areas which carry a higher risk. An example of this has been the Council investing more resources in data protection training and cyber security initiatives.

9. Phishing – In July 2022, the Council ran a phishing campaign which targeted employees for personal information. In the wider world these types of attacks continue to rise and become more sophisticated as time progresses. The simulation run by the Council was an imitation of a real attack to provide employees and Councillors with more awareness to help them stay one step ahead of real attacks.

10. Contracts – one of the most difficult areas for the Council is ensuring that external suppliers are contractually aware of their legal responsibilities when handling information on our behalf, including whether they are complying with data protection law in delivering services for the Council. All contracts issued, including the standard Terms and Conditions, contain appropriate data protection clauses. Suppliers are required to agree to these terms before we purchase from them. OneCouncil now holds in excess of 130 contract records and is now integral to all sourcing processes dealt with by the Procurement Team.

11. Data Protection Impact Assessments (DPIAs) – DPIAs are useful in helping organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. They are a statutory requirement in certain situations under GDPR and are used by the Council when there is a significant change in the way personal data is processed, such as the purchase of a new IT system. Post GDPR,

Management Team approved DPIA guidance for the Council and a number of DPIAs have now been completed since GDPR came in, including 6 more full assessments last year.

List of Appendices

Nil

Background papers:

Nil

Corporate Implications

Legal/Constitutional: These are set out in the report

Financial: None

Potential impact on climate change and the environment: None

Contribution toward achieving a net zero carbon position by 2030: None

Personnel: None

Risk Management: None

Equality and Diversity: None

Health and Safety: None

Digital: None

Other: None

Consultees: None

Relevant Policies and Strategies:

These are set out in this report